Discrete Mathematics 36 (1981) 261–271
North-Holland Publishing Company

# A GRAPH COVERING CONSTRUCTION OF ALL THE FINITE COMPLETE BIPREFIX CODES

Gerard LALLEMENT

*Department of Mathematics, Pennsylvania State University, University Park, PA 16802, USA*

Dominique PERRIN

*Université de Haute Normandie, Département de Mathématiques, B.P. 67, 76130, Mont St. Aignan, France*

Received 16 July 1980

We prove that all the finite complete biprefix codes are obtainable by realizing certain coverings of graphs of homogeneous synchronized automata by permutation groups.

A subset $C$ of the free monoid $A^*$ is called a prefix code (resp. a suffix code) if $C$ does not contain any proper left factor (resp. right factor) of a word in $C$. A code is called biprefix if it is simultaneously a prefix and a suffix code. We say that a code (prefix, suffix, or biprefix) is complete if it is maximal in its own class, under the usual inclusion of sets. By considering appropriate order relations on $A^*$, the construction of all prefix or suffix codes is quite simple. In contrast, biprefix codes, even under the additional requirement that they be finite, are much more difficult to construct. The first nontrivial construction algorithm of all finite complete biprefix codes is due to Y. Césari [1]. This algorithm, based on the fact that all these codes can be obtained from the uniform codes (codes of the form $A^n$, $n \in \mathbb{N}$) by a succession of derivations, has the disadvantage that the same biprefix code might be obtained several times. A more recent construction [2] shows how to obtain unambiguously every biprefix code of average length $n+1$ from a code of average length $n$.

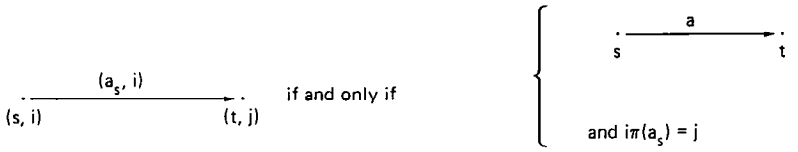
In the present paper we give a graph-theoretical construction of all finite complete biprefix codes, generalizing the concept of team tournament [4] introduced to construct all elementary codes. We show that every biprefix code of average length $n$ is obtainable from a special covering of the directed graph of a "free" synchronized homogeneous $A^*$-automation by a permutation group of degree $n$, thereby avoiding the step by step algorithm on the average length of Césari's second construction. Our algorithm is more directly related to Schützenberger's construction [7] of pairs of matrices $M, N$ such that $MP = PN$ where $P$ is the sandwich matrix of the minimal ideal of $M(C^*)$, the syntactic monoid of $C^*$.

0012-365X/81/0000–0000/$02.50 

## 1. The construction

We first recall the covering space construction of graphs due to J.L. Gross and T.W. Tucker [3]. This construction will be applied later to the state graphs of certain automata.

Let $\Gamma$ be a directed pseudograph (i.e. a graph where loops and multiple lignes are allowed), let $S$ be the set of vertices of $\Gamma$ and $W$ its set of arrows (directed edges). For a fixed set $N$, let $\pi$ be a mapping from $W$ into the symmetric group $\mathfrak{S}_N$. The covering graph $\tilde{\Gamma} = \Gamma \times_\pi N$ is the pseudograph having $S \times N$ as vertex set, and there is an arrow $(s, i) \to (t, j)$ labelled $(w, i)$ in $\tilde{\Gamma}$ if and only if $w$ is the label of an arrow $s \to t$ in $\Gamma$ and $j = i\pi(w)$. This construction (which, according to Gross and Tucker gives all the covering spaces of $\Gamma$) can be applied to the state graph of any $A^*$-automaton. Recall that a deterministic $A^*$-automaton $\mathfrak{A} = (S, f)$ is a pair consisting of a set $S$ (set of states) and a mapping $f : S \times A \to S$ (next state mapping) defining an action of the free monoid $A^*$ on $S$. The state graph of $\mathfrak{A}$ is the directed graph having $S$ as a vertex set, and there is an arrow labelled $a$ from $s$ to $t \in S$ if and only if $f(s, a) = t$. In order to make this state graph into a directed pseudograph $\Gamma$ it suffices to modify the labels of the arrows: $s \xrightarrow{a} t$ is replaced by $s \xrightarrow{a_s} t$. Any covering $\tilde{\Gamma} = \Gamma \times_\pi N$ yields then a pseudograph with arrows labelled as follows:




It is quite clear that the pseudograph $\tilde{\Gamma}$ just obtained is naturally associated with the state graph of an $A^*$-automaton $\tilde{\mathfrak{A}} = \mathfrak{A} \times_\pi N$ whose next state mapping is obtained by replacing the labels $(a_s, i)$ of $\tilde{\Gamma}$ by $a \in A$. Formally we have:

**Definition 1.1.** *Let $\mathfrak{A} = (S, f)$ be an $A^*$-automaton and let $\pi : S \times A \to \mathfrak{S}_N$ be a mapping of $S \times A$ into the symmetric group on a set $N$. The covering automaton $\tilde{\mathfrak{A}} = \mathfrak{A} \times_\pi N$ is the $A^*$-automaton $\tilde{\mathfrak{A}} = (S \times N, \tilde{f})$ where $\tilde{f}[(s, i), a] = [f(s, a), i\pi(s, a)]$.*

As usual, we shall denote $f(s, a)$ by $sa$, use the notation $a_s$ for the elements of $S \times A$ when convenient, and write the action of $A$ on $S \times N$ defined by $\tilde{f}$ simply as $(s, i)a = [sa, i\pi(a_s)]$ for every $s \in S$, $i \in N$, $a \in A$.

**Example 1.2.** If $\mathfrak{A}$ is given by the state graph $\Gamma$ below (see Fig. 1), with $N = \{0, 1, 2\}$ and $\pi(a_s) = \pi(b_s) = \pi(b_t) = (012)$, $\pi(a_t) = (01)$ we obtain $\tilde{\mathfrak{A}}$ with state graph $\tilde{\Gamma}$.

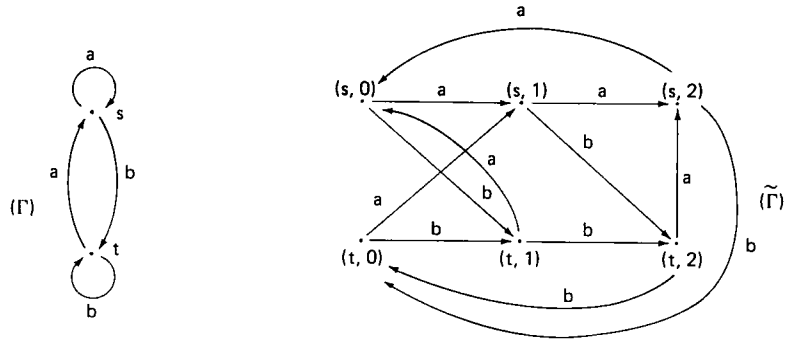



Fig. 1.

In the covering automaton $\tilde{\mathfrak{A}}$ a subset $T\times\{i\}$ of the set $S\times N$ of states is said to consist of *k-identifiable* states if $(t, i)w = (t', i)w$ for all $t, t'\in T$ and $w\in A^k$. For example the states $(s, 0)$ and $(t, 0)$ in $\tilde{\Gamma}$ above are 1-identifiable, but $(s, 1)$, $(t, 1)$ are not. It is clear that if two states $(t, i)$ and $(t', i)$ are $k$-identifiable, they are also $k'$-identifiable for any $k'\geqslant k$ and for every $a\in A$ the states $(t, i)a$ and $(t', i)a$ are $(k-1)$-identifiable.

An $A^*$-automaton $\mathfrak{A} = (S, f)$ is called homogeneous if $\mathfrak{A}$ is transitive and if there exists an integer $n$ such that all words of $A^*$ of length $\geqslant n$ define transformations of $S$ having the same rank. The smallest integer $d$ having the preceding property is called the depth of $\mathfrak{A}$. In case all words of length $\geqslant d$ define transformations of rank 1, $\mathfrak{A}$ is called homogeneous and sychronized.

**Example 1.3.** $\mathfrak{A} = (A^d, f)$ with $f(a_1a_2\cdots a_d, a) = a_2\cdots a_da$ is a homogeneous and sychronized automaton of depth $d$. Given any homogeneous synchronized $A^*$-automaton $\mathfrak{B}$ with state set $S$ and depth $\leqslant d$, the mapping $\varphi : A^d \to S$ defined by $\varphi(w) = s$ with $\{s\} = Sw$ gives a morphism from $\mathfrak{A}$ onto $\mathfrak{B}$. We shall call $\mathfrak{A}$ the *free* h.s. $A^*$-automaton of depth $d$.

For any complete finite prefix code $C$, the transition monoid $M(C^*)$ of the minimal automaton $\mathfrak{A}(C^*)$ recognizing $C^*$ admits a Suschkewitsch group $G(C^*)$ (maximal subgroup of the minimal ideal of $M(C^*)$) called the group of the code. $G(C^*)$ is in fact a permutation group acting transitively on the image of its elements viewed as transformations of the set of states of $\mathfrak{A}(C^*)$. When we refer to the degree of $G(C^*)$, it is understood as its degree as a permutation group. In case $C$ is biprefix the degree of $G(C^*)$ is also the average length of the words in $C$ with respect to any probability distribution on $A$ (see [7], [5]). It is also known in case $C$ is biprefix that $\mathfrak{A}(C^*)$ is a homogeneous automaton whose depth will be called the depth of $C$. The main result of this paper is:

**Theorem 1.4.** *Let $\mathfrak{A} = (S, f)$ be the free h.s. $A^*$-automaton of depth $d$. Construct $\tilde{\mathfrak{A}} = \mathfrak{A}\times_\pi\{0, 1, \ldots, n-1\}$, a covering automaton of $\mathfrak{A}$, satisfying the following two*

*conditions*:

(a) $S\times\{0\}$ *is a set of d-identifiable states*;

(b) *All the circuits (closed paths) in the graph* $\tilde{\Gamma}$ *of* $\tilde{\mathfrak{A}}$ *must contain a state* $(s, 0)$ *for some* $s \in S$.

*Let* $\Gamma^*$ *be the graph obtained from* $\tilde{\Gamma}$ *by merging all the states in* $S\times\{0\}$ *into a single state* $s_0$. *Then the set of all words representing minimal paths from* $s_0$ *to* $s_0$ *in the graph* $\Gamma^*$ *is a finite complete biprefix code of average length* $n$ *and depth* $\leqslant d$. *Conversely, any such code is obtainable by this construction.*

The graph $\Gamma$ of Example 1.2 is the graph of the free $A^*$-automaton of depth 1, and $\tilde{\Gamma}$ is a covering graph satisfying the conditions (a) and (b) of Theorem 1.4. Observe that the free h.s. $A^*$-automaton of depth $d$ has an arrow with label $a$ around the state $a^d$ for every $a \in A$. Condition (b) above imposes that for $s = a^d$, the permutation $\pi(a_s)$ be an $n$-cycle. Since the names of the states of $\tilde{\mathfrak{A}}$ (distinct from those in $S\times\{0\}$) do not matter, we may assume that for each $a \in A$, $s = a^d$, we have $\pi(a_s) = (0, 1, \ldots, n-1)$.

Another convention, translating condition (a) of Theorem 1.4 can be made: Let us assume, for example that we wish to construct a graph $\tilde{\Gamma}$ with $n = 4$ and $d = 2$, over an alphabet $A = \{a, b\}$. The graph of the free h.s. $A^*$-automaton $\mathfrak{A}$ of depth 2 is shown on the left in Fig. 2. A portion of the graph $\tilde{\Gamma}$ (with the convention above concerning $\pi(a)$, $\pi(b)$) appears on the right. Since the states $(a^2, 0)$, $(ba, 0)$, $(ab, 0)$, $(b^2, 0)$ must be 2-identifiable, this imposes in particular that $(ba, 0)a^2 = (a^2, 0)a^2$, hence $(ba, 0)a = (a^2, 1)$. Similarly $(ab, 0)b = (b^2, 1)$. Also $(ba, 0)b^2 = (b^2, 0)b^2 = (b^2, 2)$ forces $(ba, 0)b = (ab, i)$ to be mapped by $b$ on $(b^2, 2)$. Note that for the purpose of obtaining codes, the names of intermediate points is irrelevant, hence we may assume that $(ba, 0)b = (ab, 1)$ (i.e. $i = 1$). Similarly we put $(ab, 0)a = (ba, 1)$. Finally the states $(ba, 1)$ and $(ab, 1)$ should be mapped on states $(ab, i)$ and $(ba, j)$ by $b$ and $a$ respectively (we have chosen $i = 3$, $j = 2$ but these are determined by $\pi$). Thus the consequence of condition (a) in Theorem 1.4 is that the states $(a^2, 0)$, $(ba, 0)$ are mapped onto the same states by $a$ and $b$ respectively. The same is true for the pairs $\{(ab, 0), (b^2, 0)\}$, $\{(a^2, 1), (ba, 1)\}$, $\{(ab, 1), (b^2, 1)\}$.

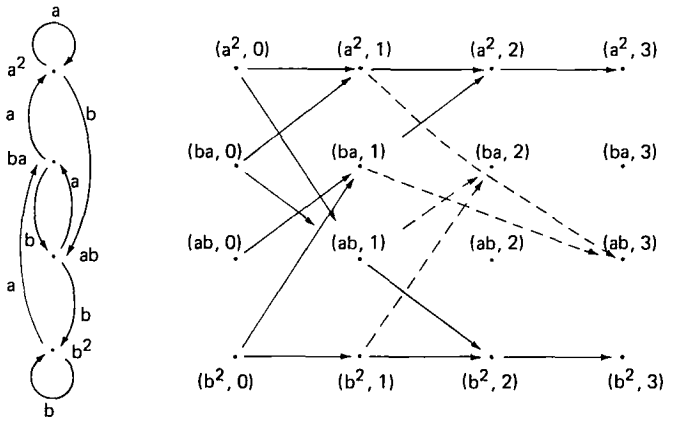



Fig. 2.

In general with $A$, $d$, $n$ arbitrary the same conventions can be adopted. In terms of the mapping $\pi$, they are: For every $a \in A$, $w \in A^d$ we have $\pi(a_w) = (0, 1, 2, \ldots, n-1)$ in case $w = a^d$, $\pi(a_w) = (0, 1, 2, \ldots i+1, \ldots) \cdots (\cdots)$ in case $w \neq a^d$ and $i$ is the largest power of $a$ which is a right factor of $w$.

Furthermore when constructing the graph $\tilde{\Gamma}$ the successive images of $(w, 0)$ must be $k$-identifiable ($d \geqslant k \geqslant 1$). This can be easily achieved by labelling identically identifiable states (see Example 1.5 below). Finally, since the graph $\Gamma^*$ is obtained from $\tilde{\Gamma}$ by merging all the states $(w, 0)$ we can systematically decide not to represent the arrows having a state $(w, 0)$ as a source or target, and read off immediately on the simplified graph of $\Gamma^*$ the biprefix code corresponding to it.

**Example 1.5.** In Fig. 3 below (completing the graph of the preceding page) we have relabelled the vertices, to show the correspondence with the usual tree

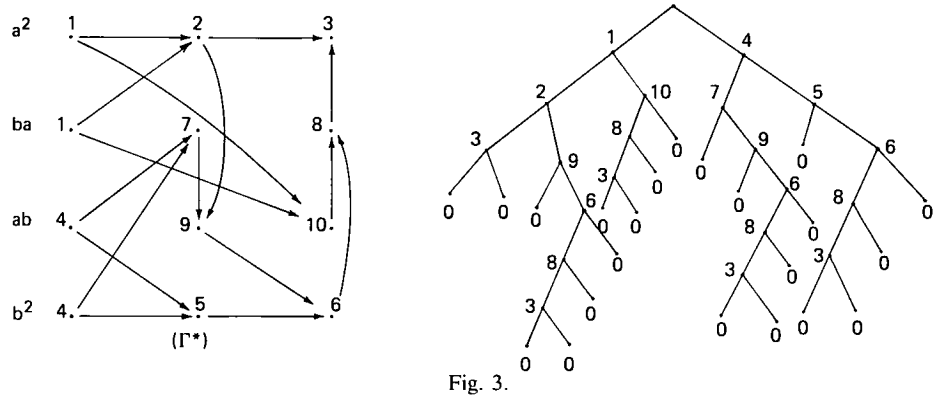



Fig. 3.

representation of the code (arrows going up are labelled $a$, arrows going down are labelled $b$)

$$C = \{a^4, a^3b, a^2ba, a^2b^2a^3, a^2b^2a^2b, a^2b^2ab, a^2b^3, aba^3,$$
$$aba^2b, abab, ab^2, ba^2, baba, bab^2a^3, bab^2a^2b, bab^2ab,$$
$$bab^3, b^2a, b^3a^3, b^3a^2b, b^3ab, b^4\} \qquad (22 \text{ words})$$

The minimal automaton recognizing $C^*$ can be obtained from the graph above by identifying the states having the same images under $a$ and $b$ (e.g. the states 6 and 10 should be identified).

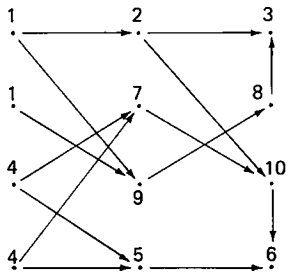


Fig. 4.

The problem of the 1–1 correspondence between the graphs and the biprefix codes is equivalent to the isomorphism problem for the central parts of the graphs. For example, the graph in Fig. 4 produces the same biprefix code as the graph $\Gamma^*$ of Example 1.5 because the central parts of the two graphs, namely


are isomorphic directed graphs, under an isomorphism ($9 \leftrightarrow 10$) that extends to the whole graphs. Once a representative of each isomorphism class of the central parts has been chosen, there is a 1–1 correspondence between the graphs and the codes. Here one must keep in mind that the construction process gives not only all the codes of degree $n$ and depth $d$, but also those of depth $< d$. In case one wishes to construct all the codes with a given underlying homogeneous synchronized automaton (homomorphic image of the free h.s. automaton), the construction can be adapted as Fig. 5 ($d = 2, n = 4$) shows.

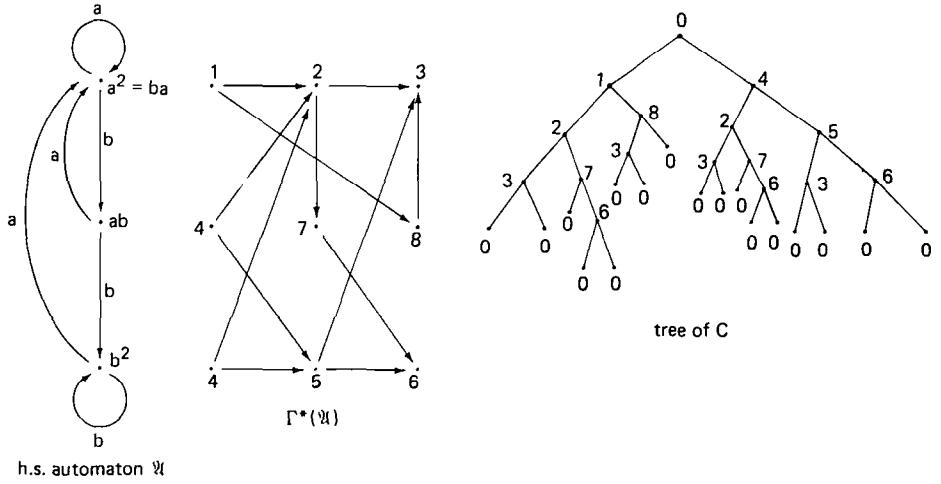



Fig. 5.

## 2. Proofs

The direct part of Theorem 1.4 follows immediately from

**Lemma 2.1.** *Let $C \subseteq A^*$ be a complete prefix rational code and let $s_0$ be the state stabilized by $C^*$ in any finite transitive $A^*$-automaton recognizing $C^*$. Then $C$ is biprefix if and only if $s_0 \in \mathrm{Im}\, w$ for all $w \in A^*$.*

**Proof.** If $C$ is a complete biprefix code, for every $w \in A^*$ there exists $v \in A^*$ such that $vw \in C^*$. Hence $s_0vw = s_0$, showing that $s_0 \in \text{Im } w$. Conversely if $s_0 \in \text{Im } w$ for all $w \in A^*$, we prove that in any transitive automaton recognizing $C^*$, $sw = s_0w$ implies $s = s_0$. Let $w' \in A^*$ be such that $sww' = s$, and let $n$ be such that $(ww')^n$ defines an idempotent transformation on the set of states. Then $s(ww')^n = s = s_0(ww')^n = s_0$ (the last equality follows from the fact that $s_0$ is in the image of the idempotent $(ww')^n$). Now if $s_0uv = s_0v = s_0$, then $s_0u = s_0$. This shows that $uv \in C^*$, $v \in C^*$ imply $u \in C^*$, or equivalently that $C$ is a suffix code. □

**Corollary 2.2.** *Let $\mathfrak{A}^*$ be the automaton obtained by merging all the states $(s, 0)$ into a single state $s_0$ in the covering automaton $\tilde{\mathfrak{A}}$ satisfying the conditions of Theorem* 1.4. *The set $C$ of all words representing minimal paths from $s_0$ to $s_0$ in the graph $\Gamma^*$ of $\mathfrak{A}^*$ is a finite complete biprefix code of average length $n$* and depth $\leqslant d$.

**Proof.** Assume that $w = a_1a_2 \cdots a_k$ with $a_i \in A$, $1 \leqslant i \leqslant k$. With the notation of Section 1 let $f(a^d, a_1a_2 \cdots a_i) = s_i$ for $1 \leqslant i \leqslant k-1$. There exists a unique sequence $i_0, i_1, \ldots, i_{k-1} \in \{0, 1, \ldots, n-1\}$ such that $i_0\pi(a^d, a_1) = i_1$, $i_1\pi(s_1, a_2) = i_2, \ldots, i_{k-1}\pi(s_{k-1}, a_k) = 0$. Then $\tilde{f}[(a^d, i_0), w] = [f(a^d, w), 0]$, showing that the image of $(a^d, i_0)$ under $w$ in $\mathfrak{A}^*$ is $s_0$. By Lemma 2.1, $C$ is biprefix. The average length of a complete biprefix code $C$ is the smallest integer $l$ such that $a^l \in C$ for every $a \in A$. This integer is precisely $n$ since $\pi(a^d, a) = (0, 1, 2, \ldots, n-1)$.

Finally, for every $s \in S$, $i \in \{0, 1, \ldots, n-1\}$ and $a_1, a_2, \ldots, a_d \in A$ we have

$$(s, i)a_1a_2 \cdots a_d = [a_1, a_2 \cdots a_d, i\pi(s, a_1)\pi(sa_1, a_2) \cdots \pi(sa_1a_2 \cdots a_{d-1}, a_d)].$$

This shows that all words of length $d$ define transformations of the same rank $n$. Hence the depth of $C$ is $\leqslant d$. □

The converse of Theorem 1.4 follows from some properties of transitive (finite) automata and biprefix codes (see [6]). Given a transitive $A^*$-automaton $\mathfrak{A} = (S, f)$, let $M$ be its transition monoid. We denote by $\mathscr{J}$ the set of all the minimal images of elements of $M$ considered as transformation on $S$, and by $\mathscr{K}$ the set of all maximal kernels of elements of $M$. For every $I \in \mathscr{J}$ and $\rho \in \mathscr{K}$, $I$ is a cross-section of $\rho$ and all $I \in \mathscr{J}$ have the same number of elements called the degree of $\mathfrak{A}$. Furthermore for $I$ and $\rho$ fixed, the set

$$G(\mathfrak{A}) = \{x \in M: \text{Im } x = I, \text{ Ker } x = \rho\}$$

is a permutation group acting transitively on $I$ called the Suschkewitsch group of $\mathfrak{A}$. We define the minimal images automaton of $\mathfrak{A}$ as the $A^*$-automaton $\mathfrak{B}$ having $\mathscr{J}$ as set of states, the action of $a \in A$ being given by $I \cdot a = f(I, a)$.

**Lemma 2.3.** *Every transitive $A^*$-automaton $\mathfrak{A}$ with state set $S$ is a homomorphic image of a covering automaton $\tilde{\mathfrak{B}} = \mathfrak{B} \times_\pi I_0$ where $\mathfrak{B}$ is the minimal images*

*automaton of* $\mathfrak{A}$ *and* $\pi : \mathscr{I} \times A \to \mathfrak{S}_{I_0}$ *is a mapping in the permutation group on a fixed minimal image* $I_0$.

**Proof.** Let $\rho_0$ be an equivalence relation on $S$ admitting every set $I \in \mathscr{I}$ as a cross-section (for example, $\rho_0 = \operatorname{Ker} w$ with $\operatorname{Im} w \in \mathscr{I}$). Define $\pi : \mathscr{I} \times A \to \mathfrak{S}_{I_0}$ as follows:

$$i\pi(I, a) = j \Leftrightarrow \begin{cases} i \equiv i' \pmod{\rho_0}, \\ i' \in I \quad \text{and} \quad i'a = j', \\ j \equiv j' \pmod{\rho_0} \end{cases}$$

for every $i \in I_0$, $I \in \mathscr{I}$, $a \in A$.

The mapping $\varphi : \mathscr{I} \times I_0 \to S$ defined by

$$\varphi(I, i) = s \quad \text{with } s \in I \text{ and } s \equiv i \pmod{\rho_0}$$

is a homomorphism from $\tilde{\mathfrak{B}} = \mathfrak{B} \times_\pi I_0$ to $\mathfrak{A}$ since $\varphi(I, i)a = sa$ with $s$ as above and $\varphi[(I, i)a] = \varphi[Ia, i\pi(I, a)] = t$ with $t \in Ia$, $t \equiv i\pi(I, a) \pmod{\rho_0}$; by definition of $\pi$, $t = sa$. Furthermore, the transitivity of $\mathfrak{A}$ implies that for every $s \in S$ there exists $J \in \mathscr{I}$ such that $s \in J$. Taking $i \in I_0$ with $i \equiv s \pmod{\rho_0}$ we have $\varphi(J, i) = s$, showing that $\varphi$ is surjective. □

**Lemma 2.4.** *Let* $C \subseteq A^*$ *be a finite complete biprefix code,* $\mathfrak{A}(C^*)$ *the minimal* $A^*$*-automaton recognizing* $C^*$*, and* $s_0$ *the state stabilized by* $C^*$ *in the set* $S$ *of states of* $\mathfrak{A}(C^*)$*. Then*

(a) $\mathfrak{A}(C^*)$ *is a homogeneous automaton of depth* $d$.

(b) *For any covering automaton* $\tilde{\mathfrak{B}} = \mathfrak{B} \times_\pi I_0$ *of the minimal images automaton* $\mathfrak{B}$ *of* $\mathfrak{A}(C^*)$ *constructed as in Lemma* 2.3, *we have*

$$C^* = \{w \in A^* : (I, s_0)w = (Iw, s_0)\}$$

*and all the states* $(I, s_0)$ *of* $\tilde{\mathfrak{B}}$ *are* $d$*-identifiable.*

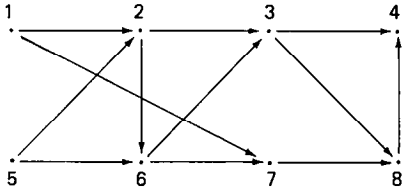
**Proof.** (a) Let $\lambda = \operatorname{Max}_{c \in C} l(c)$ and let $w \in A^*$ be any word of length $\lambda$. In order to show that the rank of $w$ is minimal, assume that $swz = twz$ for $s, t \in S$, $z \in A^*$. Since the set of states $S$ correspond to left factors of words of $C$, the fact that $l(w) = \lambda$ implies that $w = uv$ with $su = s_0$ for some $u \in A^*$. It follows that $s_0vz = suvz = swz = twz = (tu)vz$. But, as in the proof of Lemma 2.1, the fact that $s_0$ is in $\operatorname{Im} vz$ yields that $s_0 = tu$, hence $sw = s_0v = tuv = tw$, proving that $w$ has minimal rank. This shows that $\mathfrak{A}(C^*)$ is homogeneous of depth $d \leqslant \lambda$.

(b) With the notation of Lemma 2.3, for every $I \in \mathscr{I}$ and $w \in A^*$ we have $s_0\pi(I, w) = j$ where $j$ is the unique element in $I_0$ such that $s_0w \equiv j \pmod{\rho_0}$. This follows, by an easy induction on the length of $w$, from the fact that $s_0$ is in all the images (Lemma 2.1). In particular $(I, s_0)w = [Iw, s_0\pi(I, w)] = (Iw, s_0)$ if and only if $s_0 \equiv s_0w \pmod{\rho_0}$. Since $\rho_0$ admits any $I = \operatorname{Im} z (I \in \mathscr{I})$ as a cross-section this implies $s_0z = s_0wz$, thus $s_0 = s_0w$. Consequently $C^* = \{w \in A^* : (I, s_0)w = (Iw, s_0)\}$. Finally for every word $w \in A^d$, and $I, J \in \mathscr{I}$ we have $(I, s_0)w = (Iw, j)$, $(J, s_0)w =$

$(Jw, j)$ with $j \equiv s_0 w \pmod{\rho_0}$ and $Iw = Jw$ because $\mathfrak{B}$ is homogeneous synchronized of depth $d$ (i.e. words of length $d$ define transformations of rank 1 on $\mathcal{J}$). □

The converse of Theorem 1.4 follows directly from Lemma 2.4. In this Lemma it is clear that the minimal images automaton $\mathfrak{B}$ can be replaced by $\mathfrak{F}$ the free h.s. $A^*$-automaton of depth $d$, and $\mathfrak{B}$ by $\tilde{\mathfrak{F}} = \mathfrak{F} \times_{\pi_1} I_0$ with $\pi_1(w, a) = \pi(\mathrm{Im}\, w, a)$ for every $w \in A^d$.

It must be pointed out that the permutation group generated by the permutations $\pi(w, a)$, $w \in A^d$, contains, *in general strictly*, the group $G(C^*)$ of the biprefix code $C$ as the following example shows:




The graph above is a team tournament giving the permutations $\pi(a, a) = (01234) = \pi(b, b)$; $\pi(a, b) = (0134)$, $\pi(b, a) = (0123)$. These permutations correspond to the representation of $A^*$ by row-monomial matrices

$$a \to \begin{pmatrix} (01234) & 0 \\ (0123) & 0 \end{pmatrix}, \qquad b \to \begin{pmatrix} 0 & (0134) \\ 0 & (01234) \end{pmatrix}$$

obtained as in Lemma 2.3 with $I_0 = \{0, 1, 2, 3\}$ and $\rho_0 = 0|15|26|37|48$. The group $G(C^*)$ is generated by the nonzero entries of the right Schützenberger representation $\sigma$ of $M(C^*)$ using, for example $I_0 = \mathrm{Im}\, a = \{0, 1, 2, 3\}$ and $\rho_0 = \mathrm{Ker}\, a = 0|15|26|38|47$ in Lemma 2.3. This gives the representation

$$\sigma(a) = \begin{pmatrix} (01234) & 0 \\ (01234) & 0 \end{pmatrix}, \qquad \sigma(b) = \begin{pmatrix} 0 & (014) \\ 0 & (01243) \end{pmatrix}.$$

$G(C^*)$ is the alternating group $\mathfrak{A}_5$ and the permutations $\pi$ generate $\mathfrak{S}_5$.

In order to obtain the generators of the group $G(C^*)$ of the code, it suffices in the proof of Lemma 2.3 to replace $\rho_0$ by an equivalence $\rho_1$ which is a maximal kernel for $\mathfrak{A}(C^*)$. We denote by $\sigma_0$ the representation of $A^*$ by row-monomial matrices over $\mathfrak{S}_{I_0} \cup \{0\}$ deduced from Lemma 2.3 and $\sigma_1$ the similar representation using $\rho_1$ instead of $\rho_0$. For every $a \in A$, $\nu = 0, 1$

$$[\sigma_\nu(a)]_{I,J} = \begin{cases} \pi_\nu(I, a) & \text{if } J = Ia, \\ 0 & \text{otherwise} \end{cases}$$

and $i\pi_\nu(I, a) = j$ if and only if $i \equiv i' \pmod{\rho_\nu}$, $i' \in I$, $j \equiv j' \pmod{\rho_\nu}$, $i'a = j'$. For every $I \in \mathcal{I}$ define $\chi_I \in \mathfrak{S}_{I_0}$ by

$$i\chi_I = j \Leftrightarrow i \equiv i' \pmod{\rho_1},\ i' \in I,\ i' \equiv j \pmod{\rho_0}.$$

Let $\chi$ be the $\mathcal{I} \times \mathcal{I}$ diagonal matrix over $\mathfrak{S}_{I_0} \cup \{0\}$ having $\chi_I$ in position $(I, I)$.

**Property 2.5.** $\sigma_1 = \chi\sigma_0\chi^{-1}$.

**Proof.** We show that $\chi\sigma_0(a) = \sigma_1\chi(a)$ for every $a \in A$. The entry in position $(I, Ia)$ of $\chi\sigma_0(a)$ is $\chi_I\pi_0(I, a)$, while the entry in the same position in $\sigma_1\chi(a)$ is $\pi_1(I, a)\chi_{Ia}$. Assume that for $i, j \in I_0$ we have $i\chi_I\pi_0(I, a) = j$. Then $i\chi_I = k$, $k\pi_0(I, a) = j$. Hence $i \equiv i' \pmod{\rho_1}$, $i' \in I$, $i' \equiv k \pmod{\rho_0}$ and $k \equiv i' \pmod{\rho_0}$ with $i' \in I$, $i'a = j' \in Ia$, and $j' \equiv j \pmod{\rho_0}$. Then it follows that $i\pi_1(I, a) = j_1$ with $j_1 \equiv j' \pmod{\rho_1}$; furthermore $j_1\chi_{Ia} = j$ since $j_1 \equiv j' \pmod{\rho_1}$, $j' \in Ia$, and $j' \equiv j \pmod{\rho_0}$; hence $i\pi_1(I, a)\chi_{Ia} = j$. Since $\chi_I\pi_0(I, a)$ and $\pi_1(I, a)\chi_{Ia}$ are permutations, this is enough to ensure $\chi_I\pi_0(I, a) = \pi_1(I, a)\chi_{Ia}$. □

When constructing the automaton $\mathfrak{A}^*$ obtained from $\tilde{\mathfrak{A}}$ (Theorem 1.4) by merging all the states $(s, 0)$ into a single state we construct simultaneously the permutations $\pi_0(s, a)$ for $s \in A^d$, $a \in A$ and the equivalence $\rho_0$. We have $i\pi_0(s, a) = j$ if and only if there is an arrow labelled $a$ from $(s, i)$ to $(sa, j)$ in the graph $\Gamma^*$. The minimal images of $\mathfrak{A}$ are $I_s = \{(s, i): i = 0, 1, \ldots, n-1\}$ and if $I_0$ is chosen to be the image of $a^d$ for some fixed letter $a \in A$ we have $(s, i)\rho_0(t, j)$ if and only if $i = j$. Indeed, if $\pi$ is the permutation on $\operatorname{Im} a^d$ defined as in Lemma 2.3 (using $\rho_0$ above) we have

$$(a^d, i)\pi(I_s, b) = (a^d, j) \quad \text{with } (a^d, i) \equiv (s, i) \pmod{\rho_0},$$
$$(s, i)b = (sb, i\pi_0(I_s, b)) \quad \text{and} \quad (sb, i\pi_0(I_s, b)) \equiv (a^d, i\pi_0(I_s, b))$$

Hence $j = i\pi_0(I_s, b)$, showing that $(s, i)\rho_0(t, j)$ iff $i = j$.

Using $\rho_1 = \operatorname{Ker} a^d$ as equivalence we obtain: $(s, i)\rho_1(t, j)$ if and only if $(s, i)a^d = (t, j)a^d$ or equivalently

$$i\pi_0(s, a^d) = j\pi_0(t, a^d)$$

Computing $\chi_{I_s}$ we obtain

$$\chi_{I_s} = \pi_0(a^d, a^d)[\pi_0(s, a^d)]^{-1},$$

and applying Property 2.5 gives the generators of the group $G(C^*)$

$$\pi_1(s, b) = \pi_0(a^d, a^d)[\pi_0(s, a^d)]^{-1}\pi_0(s, b)\pi_0(sb, a^d)[\pi_0(a^d, a^d)]^{-1}$$

Note that $\pi_0(a^d, a^d) = (0, 1, 2, \ldots, n-1)^d$.

In conclusion, we recall that the number of codes of a given length is finite (see [2], for example). Hence the depth $d$ is bounded by a function of $n$. As long as

$d \leqslant 5$ we have $d \leqslant n$, however we have constructed a code of length 10 and depth 14. The determination of the nature of $f$ such that $d \leqslant f(n)$ seems to be a difficult problem.

## References

[1] Y. Césari, Sur un algorithme donnant les codes bipréfixes finis, Math. Syst. Th. 6 (1972) 221–225.
[2] Y. Césari, Propriétés combinatoires des codes bipréfixes complets finis, in "Théorie des Codes", Actes de la septième Ecole de Printemps d'Informatique Théorique, Jougne 1979, 29–46.
[3] J.L. Gross and T.W. Tucker, Generating all graph coverings by permutation voltage assignments, Discrete Math. 18 (1977) 273–283.
[4] G. Lallement and C. Reis, Team tournaments and finite elementary codes, to appear in Information and Control.
[5] D. Perrin, Codes bipréfixes et groupes de permutations, Doctoral Thesis University of Paris, 1975.
[6] D. Perrin, La représentation ergodique d'un automate fini, Theoret. Comput. Sci. 9 (1979) 221–241.
[7] M.P. Schützenberger, On a special class of recurrent events, Ann. Math. Stat. 32 (1961) 1201–1213.